NAWCWDINST 5211.1
730000D
27 Sep 2001

NAWCWD INSTRUCTION 5211.1

From: Commander, Naval Air Warfare Center Weapons Division

Subj: PERSONAL PRIVACY AND RIGHTS OF INDIVIDUALS REGARDING THEIR PERSONAL RECORDS

Ref: (a) Public Law 93-579, The Privacy Act of 1974
(b) SECNAVINST 5211.5D

1. Purpose. To carry out the provisions of the Privacy Act of 1974 and related directives and emphasize the requirements for safeguarding of records covered by the Privacy Act. This revision provides current guidelines regarding types of information that may be disclosed, defines what constitutes a violation of the Privacy Act, and provides guidance for disposal of records protected by the Privacy Act.

2. Cancellation. NAVWPNCENINST 5211.2B.

3. Scope. The Privacy Act is applicable to all U.S. citizens and to aliens lawfully admitted for permanent residence. This instruction applies to employees paid from appropriated and non-appropriated funds, contractor personnel, and other individuals (e.g., job applicants) about whom personal data records are maintained.

4. Definitions

a. A personal data record is defined in the Privacy Act as any item, collection, or grouping of information about an individual, including but not limited to, education, financial transactions, medical history, and criminal or employment history that contains the individual's name, social security number, or other identifying number or symbol.

b. A system of records, as referred to in this instruction, is defined as a group of records under the control of a federal agency from which information is retrieved by the name of the individual or by some identifying number or other identifying symbol.

5. Background

a. Reference (a) establishes the right to privacy as a personal and fundamental right protected by the Constitution of the United States. It:

(1) Prescribes what records agencies may keep that contain personal information.

(2) Requires public notice as to what records are being kept in a system of records and why.

(3) Allows individuals access to their own records and an opportunity to challenge the accuracy of the records.

(4) Deals with the security of these records, including their release to other parties.

b. In addition, reference (a) requires that when personal data is requested for a system of records from employees, either verbally or by means of a form, each employee must be given a written statement advising him or her of:

(1) The authority (statute or Executive Order) for requesting the data.

(2) The purposes for which it is requested.

(3) The use to be made of the data.

(4) Whether it is mandatory to provide the data.

(5) What the consequences are of not providing the data.

c. Reference (b) states Department of the Navy (DON) policies, rules, procedures, and requirements for implementation of the Privacy Act.

6. Exceptions. Some systems of records are exempt from certain provisions of the Privacy Act. Generally, these records systems fall into the following categories:

a. Certain law enforcement records (e.g., Central Intelligence Agency and Federal Bureau of Investigation records, records identifiable to an individual compiled in the enforcement or investigation of a criminal matter, or both).

b. Classified national defense information.

c. Certain test and examination material such as that used solely to determine individual qualifications for appointment or promotion.

d. Certain investigatory records such as suitability determinations, eligibility or qualifications for federal civilian employment, military service, federal contracts, or access to classified information.

7. Policy

a. Departments will only keep personal information concerning individuals that managers determine to be reasonably necessary to accomplish their assigned functions, and will maintain only those records systems that have had a description published in the Federal Register.

(1) The DON has published, in the Federal Register, general and specific descriptions of numerous records systems including those typically maintained by field activities; e.g., personnel, payroll, security, housing, safety, etc. If you have any question as to whether a given department or supervisor is authorized to keep a certain kind of record containing personal data, contact the Naval Air Warfare Center, Weapons Division Privacy Act Coordinator, Code 731000D.

(2) Activities cannot maintain personnel records describing how individuals exercise rights guaranteed by the First Amendment (e.g., religious and political beliefs, freedom of speech and the press, freedom of assembly and petition, etc.), unless they are specifically authorized by statute or by the individual concerned, or are within the scope of an authorized law enforcement activity. However, the Privacy Act does not preclude maintaining such information in personnel records if it is given voluntarily by the individual concerned.

(3) Activities will make every reasonable effort to assure that personal data records maintained are as accurate, relevant, timely, and complete as necessary to ensure fairness in any determinations made on the basis of the records.

b. When an individual requests access to information or when an individual requests to amend information contained in a system of records, the following will apply:

(1) An individual, before being given notification or being granted access to personal information, must either be known or provide verification of his or her identity; acknowledge requests for access to records within 10 working days of receipt; and provide access to records, if appropriate, within 30 working days.

(2) An individual may designate one person to accompany him or her when inspecting the record.

(3) An individual must be furnished with the record in a form comprehensible to the individual (e.g., coded computer produced data should be decoded or translated).

(4) An individual may obtain a copy of the record for a fee equal to the duplication fees. However, charges may and should be waived in cases where the records are not large. No fees may be charged for search for and retrieval of the records, review of the records, or making a copy of a record when it is a necessary part of the process of making the record available for review.

(5) An individual's medical record will be disclosed to the individual to whom it pertains unless, in the judgment of a physician, access to such record could have an adverse effect on the individual's physical or mental health. When such a judgment is made, the individual will be asked to name a physician to whom the information will be transmitted.

(6) An individual given access to his or her own records, must not be given information pertaining to other individuals in that records system.

(7) Before an individual is denied access to his or her records or is denied access to make an amendment to his or her records, consult the Privacy Act Coordinator, Code 731000D, for guidance. The Privacy Act Coordinator will determine the appropriateness and the proper procedures for exercising such a denial.

NOTE: The procedures listed in paragraphs 7b(1) – 7b(7) pertain to all systems of records other than those specified in paragraph 6.

c. No record contained in a system of records will be disclosed without prior written consent of the individual concerned unless disclosure falls into one of the following areas:

(1) Request is made by personnel of the DON or Department of Defense , or both, who have a need-to-know in the performance of their official duties and when the use if compatible with the purpose for which the record is maintained.

(2) Information is releasable under the Freedom of Information Act. For example, for a specifically identified current or former civilian employee: Name, present and past position titles, grades, salaries, dates of employment, duty station (building and/or department), office telephone number, and address. For military personnel: Name, rank or rate, date of rank, salary, present and past duty stations, final duty station, office telephone number, source of commission, military and civilian educational level, and promotion sequence number.

(3) Record is required for routine use as described for that particular system of records in the Federal Register. Normally, this refers to interagency transfers of records such as the transfer of certain payroll data to the Internal Revenue Service and state taxing authorities.

(4) Request is made by the Bureau of Census. (Consult Code 731000D personnel on such inquiries.)

(5) There is statistical research or reporting in a form where the identity of individuals cannot be used.

(6) Request is made by the National Archives. (Consult Code 731000D personnel on such inquiries).

(7) Record is required by civil or criminal law enforcement agencies. These requests must be made in writing by a supervisory official and must specify the particular record desired and the law enforcement purpose for which the record is sought. Blanket requests for all records pertaining to an individual will not be honored.

(8) There is an emergency condition involving compelling circumstances affecting the health and safety of a person.

(9) Record is requested by Congressional committees, sub-committees, or joint committees (but not individual congressmen).

(10) Request is made by the Comptroller General. (Consult with Code 731000D personnel on such inquiries.)

(11) There is a court order. Notification must be made to the individual to whom the record pertains if the order is a matter of public record. If the order is not a matter of public record, this activity must seek to be informed as to when it will become public and at the time notify the individual of the disclosure.

d. Except for disclosure of information made under paragraphs 7c(1) and 7c(2) above, an accounting must be kept of the date, nature, and purpose of each disclosure of a record to any person or organization, even if the disclosure is consented to or requested by the individual. The accounting must include the name and address of the person or organization to whom the disclosure is made. The record of accounting must be retained for at least five years after the last disclosure or the life of the record, whichever is longer. Recipients of information subsequently amended must be supplied with the amendments.

e. Administrative, technical, and physical safeguards must be established to ensure the security and confidentiality of records. Civil Service personnel records must be maintained in a lockable metal file cabinet or secured room when not in the custody of an authorized person.

f. When a form, questionnaire, report, or other media (such as an interview) is used to collect personal data from an individual for a system of records, the individual must first be given a written Privacy Act Statement advising him or her of the following: the statute or Executive Order authorizing the solicitation; the major purposes and routine uses of the information; and whether disclosure is voluntary or mandatory and the possible consequences for failing to respond.

(1) If an individual is requested to disclose his or her Social Security Number (SSN), the Privacy Act Statement must also inform him or her whether such disclosure is mandatory or voluntary, by what statute or other authority the number is solicited, and what uses will be made

of it. An individual may not be denied any right, benefit, or privilege provided by law because the individual refuses to disclose his or her SSN, unless such disclosure is required by federal statute or, in the case of systems of records in existence and operating before 1 January 1975, where such disclosure was required under statute or regulation adopted before 1 January 1975 to verify identity.

(2) A Privacy Act Statement is not required if the information is not solicited from the individual (for example, if it is obtained from other records).

8. Records Disposal. Take reasonable care to ensure that unauthorized disclosure of Privacy Act data does not occur during records disposal. Tear paper records into small pieces or shred and place in regular trash containers. Bulky records may be burned. Deface data (other than paper records) in such a way as to preclude unauthorized disclosure.

9. Penalties. The Privacy Act provides for criminal sanctions and fines up to $5,000 against officials or employees who:

a. Willfully disclose information protected under the Privacy Act to an individual or agency not authorized access to it.

b. Willfully maintain a system of records that was not published in the Federal Register.

c. Willfully receive personal data under false pretenses. Willfully is defined as a voluntary and intentional disclosure.

10. Action

a. Supervisors, managers, and all other employees within their respective organizations, are responsible for carrying out the provisions of the DON's privacy program, as given in this instruction and in reference (b). Managers of Privacy Act information are responsible for conducting periodic compliance evaluations.

b. The Privacy Act Coordinator, Code 731000D, is available for advice and assistance on all matters relating to the Privacy Act and its implementation.

11. Directive Responsibility. The Head, Personnel Department, Code 730000D, is responsible for keeping this instruction current.

/s/
M. J. SWANEY